A Secure Localization Algorithm Based on Confidence Constraint for Underwater Wireless Sensor Networks

Xiaofeng Xu[1], Guangyuan Wang[2], Yongji Ren[3(✉)], and Xiaolei Liu[4]

[1] Science and Technology on Communication Information Security Control Laboratory, Jiaxing 314033, China
[2] Department of Military Training, Naval Aeronautical and Astronautical University, Yantai 264001, China
[3] Department of Command, Naval Aeronautical and Astronautical University, Yantai 264001, China
lenglengqiuyu@sina.com
[4] Department of Electrical Engineering, Yantai Vocational College, Yantai, 264001, China

Abstract. This paper proposed a novel secure localization algorithm based on confidence constraint for Underwater Wireless Sensor Networks (UWSNs). In recent years, UWSNs have attracted a rapidly growing interest from ocean battlefield surveillance. As essential technology, secure localization is crucial to the location-based applications. However, the localization process has been restricted by the adverse battlefield environments, e.g. the confidence problem of reference nodes and information due to disturbances or attacks, which lead to obvious degradation of localization security and accuracy. To solve this issue, we transformed the secure localization into a confidence constraint satisfaction problem. Zero-sum game method has been utilized to deal with the confidence problem of reference information. Simulation results show that our algorithm is an effective and efficient approach to localization for UWSNs.

Keywords: UWSNs · Localization · Security · Confidence constraint

1 Introduction

During the last few years, there has been a rapidly growing interest in Underwater Wireless Sensor Networks (UWSNs), which brought us a new way to sense and monitor the adverse battlefield environments [1]. As an essential technology, the localization performance significantly affects the location-based applications. In complex ocean battlefield, several kinds of adverse factors would lead to obvious degradation of localization security and accuracy [2], e.g. the potential malicious attacks, the unreliable reference nodes and reference information, etc. Extensive research has been conducted in this interesting area [3–5]. Therein, Alfao et al. considered the security of localization under limited trust anchor nodes [4]. It introduced three algorithms to enable the sensor nodes to determine their positions. But it would fail when the malicious anchor nodes are in colluding condition. Chen et al. proposed to make each locator build a conflicting-set and then the sensor can use all conflicting sets of its neighboring locators to exclude

K. Kim and N. Joukov (eds.), *Information Science and Applications 2017*,
Lecture Notes in Electrical Engineering 424, DOI 10.1007/978-981-10-4154-9_6

incorrect distance measurements of its neighboring locators [5]. However, the limitation of the scheme is that it only works properly when the system has no packet loss.

Actually, the substantial reason of the above problem is that the localization has been restricted by confidence constraint of reference information. Therefore, a novel secure localization algorithm based on confidence constraint has been proposed. We transformed the secure localization problem into a confidence constraint satisfaction problem (CSP) [6]. A confidence CSP, i.e. the determination problem of secure localization, has been defined by a constraint contractor C, with an interval domain $[x]$. Then, the localization issues will be tackled in a constraint CSP framework.

2 Confidence Constraint Based Secure Localization Algorithm

2.1 Confidence Constraint of Reference Nodes

In this phase, our primary objective is to find out which anchor nodes should be employed as reference nodes so that the utilization in localization is secure. To deal with the problem, zero-sum game method will be employed [7].

Formulate game domain. Firstly, the ordinary node N_i initiates an inviting request to its neighbor or multi-hop anchor nodes, namely set X. If the anchors in X are overcommitted, they respond the abandoning ACK to N_i. Otherwise, the nodes respond the joining ACK. Then the local game domain of node N_i is created, and the anchors with joining ACK will become the game players. As a game player, there are two actions <keep, reject> to enforce for N_i. Assume that the UWSN is composed by n nodes and m game domains acting on it. Note that the m game domains could co-exist over the network so that the game-plays could be calculated in the concurrent way.

Calculate cost functions. The node N_i announces the localization information to all the players. Then, each player in the local game domain receiving the announcement calculates its cost function [8]. The cost function of game domain k is given by

$$J^k\left(t,x,u^k\right) = \int_t^{t_f} L^k\left(t,x,u^k\right)dt + \Psi^k\left(x_{t_f}^k\right), \quad 1 \le k \le m \tag{1}$$

with the running cost function

$$L^k\left(t,x,u^k\right) = \sum_{i\in V_k} c_i\left(u_i\right) - \sum_{i\in V_k}\sum_{j\in V_{k',k'\neq k}} \left[a_{i,j}e^{-\theta_{i,j}^k\left(x_{i,r_{l_k}} - x_{j,r_{l_k}}\right)} - a_{i,j}e^{-\omega_{i,j}^k\left(x_{i,r_n} - x_{j,r_n}\right)}\right] \tag{2}$$

where x_i describes the running states of N_i, u^k describe the control vectors of group k, V_k is the node set and Ψ^k is the terminal cost function. c_i is control cost function of node N_i. $a_{i,j}e^{-\theta_{i,j}^k}$ are attack payoffs running functions and $a_{i,j}e^{-\omega_{i,j}^k}$ are information loss running functions of node N_i to N_j.

Play game and make decision. At the first time of the play, all players make their action based on their payoffs, i.e. if the payoff is positive, broadcasting a 'keep' message to all players, or else broadcasting 'reject'. All localization groups wish to maximize their payoffs, i.e. minimize the respective cost functions. Let group k's admissible control set be u^k. As the game repeats, the admissible control combination, i.e. the actions of game-play, can be denoted as a Nash equilibrium solution if it satisfies:

$$J^k\left(0, x, u^k\right) \leq J^k(0, x, \langle \hat{u}|k \rangle), \quad 1 \leq k \leq m \tag{3}$$

On this basis, the ordinary node can adopt the players with 'keep' as the reference anchors, and then broadcasts a message to all players to dismiss the game domain.

2.2 Confidence Constraint Satisfaction Problem

Solving the confidence CSP in an interval analysis approach consists of finding the intersection that contains all possible solutions. The set of the intervals regarding to ordinary node N_i actually is the set of the constraints $f_1, f_2, \cdots, f_k$. The location of node N_i can be described by $\boldsymbol{X}_i = [x_i, y_i, z_i]^T$. The distance from X_u to X_i can be denoted by $\zeta_{ui}^I = \left[\zeta_{ui}^{I-}, \zeta_{ui}^{I+}\right]$. Consider the intersection of two intervals ζ_{u1}^I and ζ_{u2}^I, it can be computed by $\zeta_{u1}^I \cap \zeta_{u2}^I = \left[max\left\{\zeta_{u1}^{I-}, \zeta_{u2}^{I-}\right\}, min\left\{\zeta_{u1}^{I+}, \zeta_{u2}^{I+}\right\}\right]$. The admissible solutions of node X_u can be rewritten as $F_u = \bigcap_{i=1}^{k} \left\{\zeta \in \zeta^I : \zeta_{ui}^I = \left[\zeta_{ui}^{I-}, \zeta_{ui}^{I+}\right]\right\}$. Regarding the coordinates of all sub-boxes' centers as samples of X_u, we can get a sample set $F_u = \left\{\Theta_1, \Theta_2, \cdots, \Theta_n\right\}$, and the centre of Θ_n can be found by $\zeta_n^* = (\zeta_n^- + \zeta_n^+)/2$. Then the optimum point estimate, i.e. the desired coordinates of ordinary node X_u can be obtained by $\hat{\boldsymbol{W}}_u = \arg\min_{W_u} \sum_{i=1}^{k} \left(\left\|\zeta_n^* - \boldsymbol{W}_i\right\|_2 - d_{ui}\right)^2$.

3 Performance Evaluation

In our simulation experiments, 400 nodes with adjustable transmission range R are randomly distributed in a $3000 \times 3000 \times 200$ region. For comparison with classical approaches relying on secure hypotheses, different effective reference anchor percentages are considered in our simulation by varying the malicious nodes percent. Moreover, the DV-distance localization scheme has been simulated for comparison.

Figure 1 shows the accuracy comparisons with different anchors. When we varied the effective anchor percentage from 4% to 12%, i.e. the number of effective anchor nodes varying from 16 to 48, the localization error decreased by 50%. However, the DV-distance scheme only decreased by 25%, when the network connectivity is 9 and the malicious nodes percent is 5%. This suggests that our scheme can achieve higher localization accuracy and security in same malicious nodes percentage.

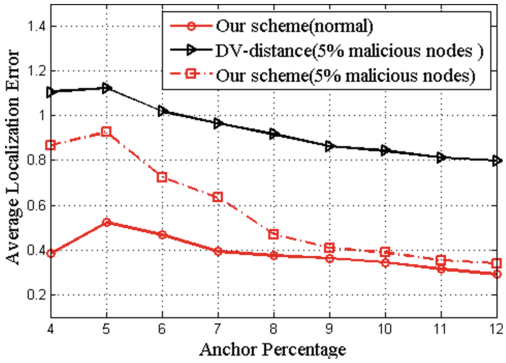

Fig. 1. Average localization error vs. anchor number

Conclusion. Proposed is a novel confidence constraint based secure localization algorithm. The advantage of our framework is that both the malicious nodes and the reference information can be treated as information uncertainty and casted into game process. Simulation results show that it is an effective and efficient approach.

Acknowledgment. This work was supported by the National Natural Science Foundation of China (grant no. 61501488).

References

1. Erol-Kantarci, M., Mouftah, H.T., Oktug, S.: A survey of architectures and localization techniques for underwater acoustic sensor networks. Commun. Surv. Tutorials IEEE **13**(3), 487–502 (2011)
2. Tan, H., Diamant, R., Seah, W.K.G., Waldmeyer, M.: A survey of techniques and challenges in underwater localization. Ocean Eng. **38**(14–15), 1663–1676 (2011)
3. Xing, T., Jian, L.: Cooperative positioning in underwater sensor networks. IEEE Trans. Signal Process. **58**(11), 5860–5871 (2010)
4. Alfao, J.G., Barbeau, M., Kranakis, E.: Secure localization of nodes in wireless sensor networks with limited number of truth tellers. In: Proceedings of 7th Annual Communication Networks and Services Research Conference, pp. 86–93 (2009)
5. Chen, H., Lou, W., Wang, Z.: Conflicting-set-based wormhole attack resistant localization in wireless sensor networks. In: Proceedings of the 6th International Conference on Ubiquitous Intelligence and Computing, pp. 296–309 (2009)
6. Jaulin, L., Kieffer, M., Didrit, O., Walter, E.: Applied Interval Analysis, with Examples in Parameter and State Estimation, Robust Control and Robotics. Springer, London (2001)
7. Cheng, G., Chen, H.: Game model for switch migrations in software-defined network. Electron. Lett. **50**(23), 1699–1700 (2014)
8. Ning, G., Yang, D., Tie, L., Cai, K.-Y.: Nash equilibrium of time-delay interaction complex networks subject to persistent disturbances. IET Control Theory and Applications (2012)